El sitio web oficial del proyecto de criptomonedas Monero, fue hackeado y los responsables del ataque reemplazaron de forma silenciosa los binarios legítimos de Linux y Windows disponibles para descargar versiones maliciosas diseñadas para robar fondos de las billeteras de los usuarios.

El último ataque cibernético a la cadena de suministro se reveló el lunes luego de que un usuario de Monero descubriera que el hash criptográfico de los archivos binarios que se descargó del sitio oficial, no coincidía con los hash enumerados en él.

Después de una investigación, el equipo de Monero confirmó que su sitio web, GetMoneto.com, estaba comprometido, lo que podría afectar a los usuarios que descargaron la billetera CLI entre el lunes 18 a las 2:30 am y 4:30 pm UTC.

Hasta ahora, no se sabe cómo los atacantes lograron comprometer el sitio web de Monero y cuántos usuarios se vieron afectados y perdieron sus fondos digitales.

Según un análisis de los archivos binarios maliciosos realizado por el investigador de seguridad BartBlaze, los atacantes modificaron archivos binarios legítimos para inyectar algunas funciones nuevas en el software que se ejecuta después de que un usuario abre o crea una nueva billetera.

Las funciones maliciosas están programadas para robar y enviar automáticamente el seed de la billetera de los usuarios, una especie de clave secreta que restaura el acceso a la billetera, a un servidor remoto controlado por el atacante, lo que permite a los hackers robar fondos sin problemas.

> *«Hasta donde puedo ver, no parece crear ningún archivo o carpeta adicional, simplemente roba su semilla e intenta extraer fondos de su billetera»,* dijo el investigador.

Un usuario de GetMonero en Reddit afirmó haber perdido 7000 dólares en Monero después

de instalar el binario malicioso de Linux.

> *«Puedo confirmar que el binario malicioso está robando monedas. Aproximadamente 9 horas después de ejecutar el binario, una sola transacción agotó mi billetera de todos los $7000»,* dijo el usuario.

Los funcionarios de GetMonero aseguraron a sus usuarios que los archivos comprometidos estuvieron en línea por un período de tiempo muy corto y que los archivos binarios ahora se brindan desde otra fuente segura.

Además, aconsejaron encarecidamente a los usuarios que revisen los hash de sus archivos binarios para el software CLI de Monero y eliminen los archivos si no coinciden con los oficiales.

> *«Se recomienda encarecidamente a cualquiera que descargue la billetera CLI de este sitio web entre el lunes 18 a las 2:30 am UTC y las 4:30 pm UTC, que revise los hash de sus binarios»,* dijo GetMonero.